

FIG. 1

FIG. 1 is a block diagram of a network architecture. The network architecture includes a fabric 102, a user interface 142, a storage device 170, a logical unit 172, a logical unit 174, a private loop 122, a public loop 162, a database 132, and a tablet 134. The fabric 102 includes switches 110, 112, 114, and 116. The private loop 122 includes server racks 124 and 126. The public loop 162 includes server racks 164, 166, and 168. The database 132 and tablet 134 are connected to switch 110. The user interface 142 is connected to switch 112. The storage device 170 is connected to switches 112 and 114. The logical unit 172 is connected to switch 114. The logical unit 174 is connected to switch 116. The private loop 122 is connected to switch 110. The public loop 162 is connected to switch 116.

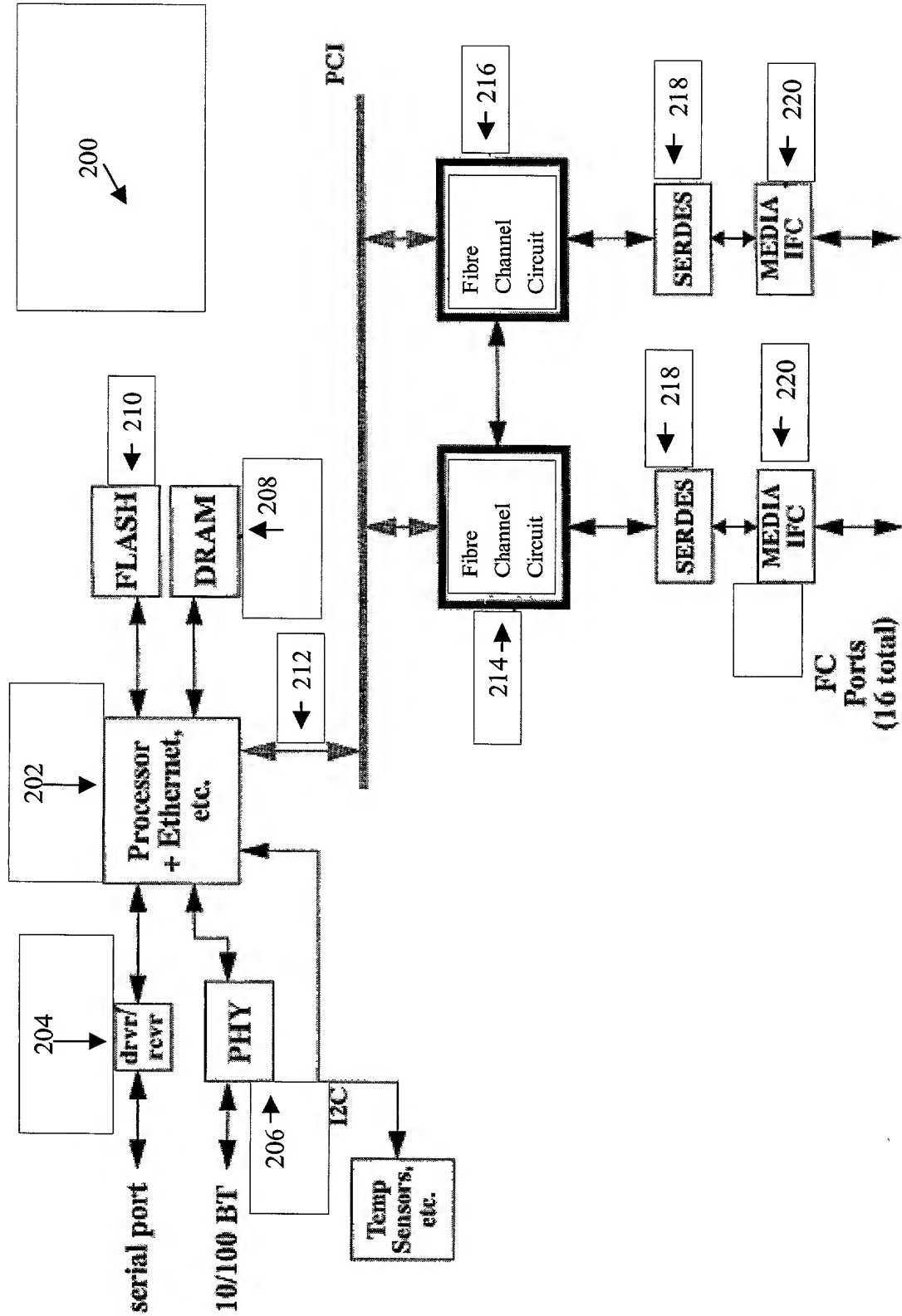


Figure 2

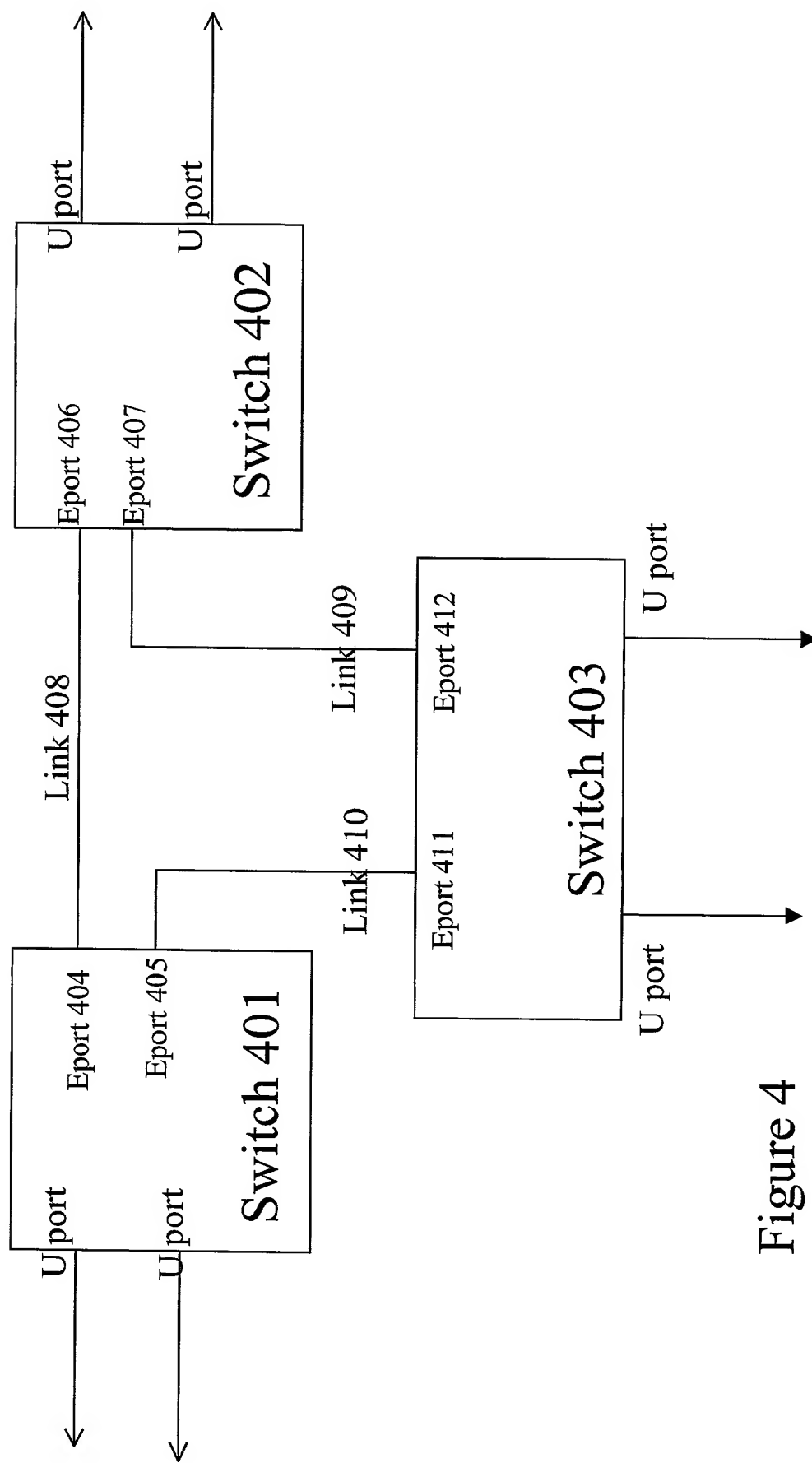


Figure 4

504 Fact-A
504 Fact-A
505 InfoB
506 - Derivative of InfoB

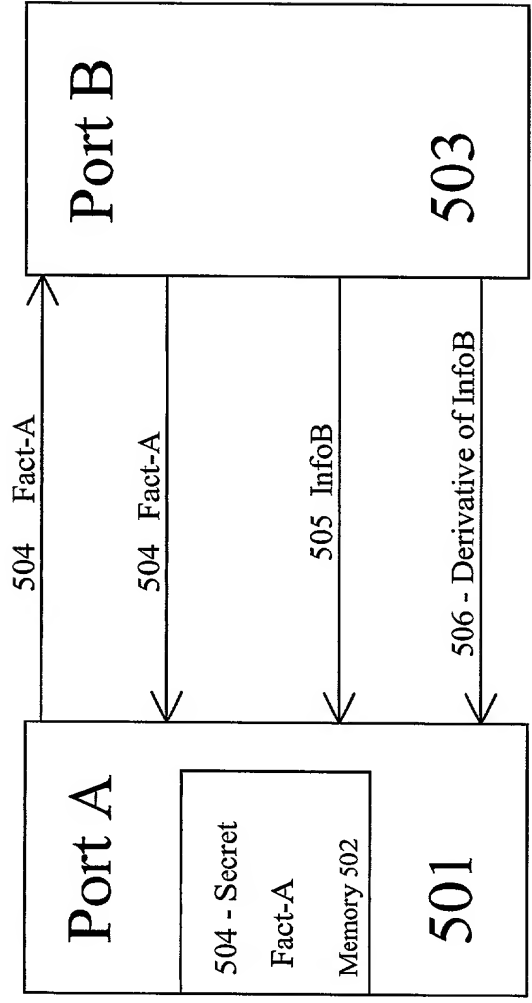


Figure 5a

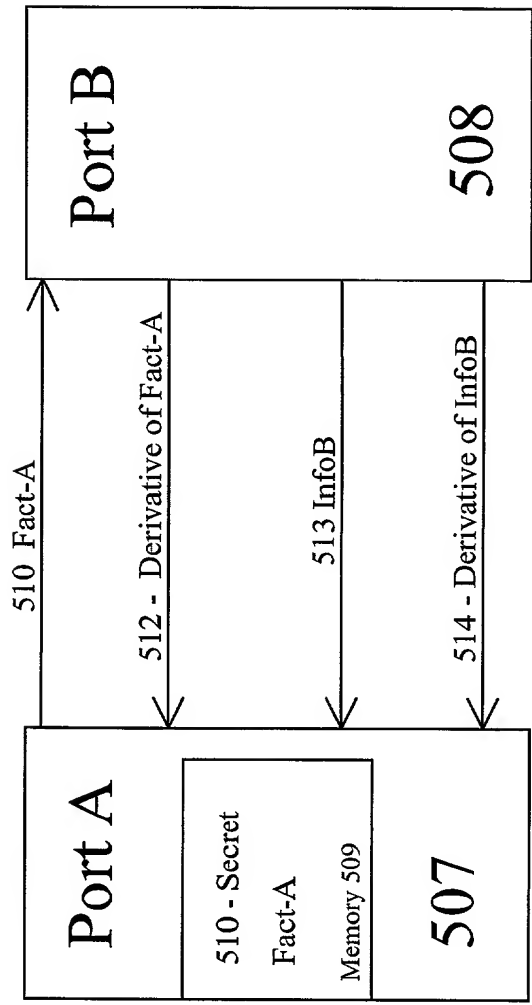


Figure 5b

US 2017/0104000 A1
FIG. 5c

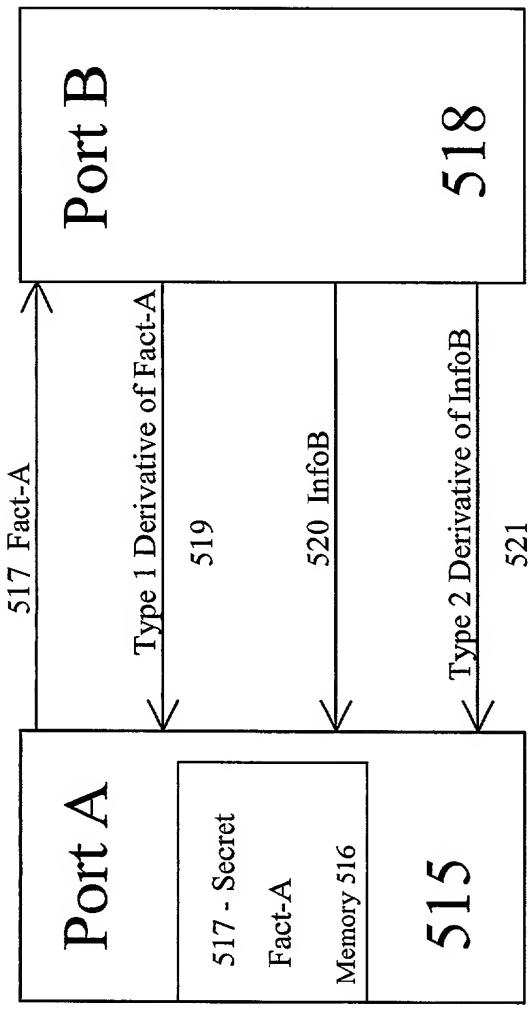


Figure 5c

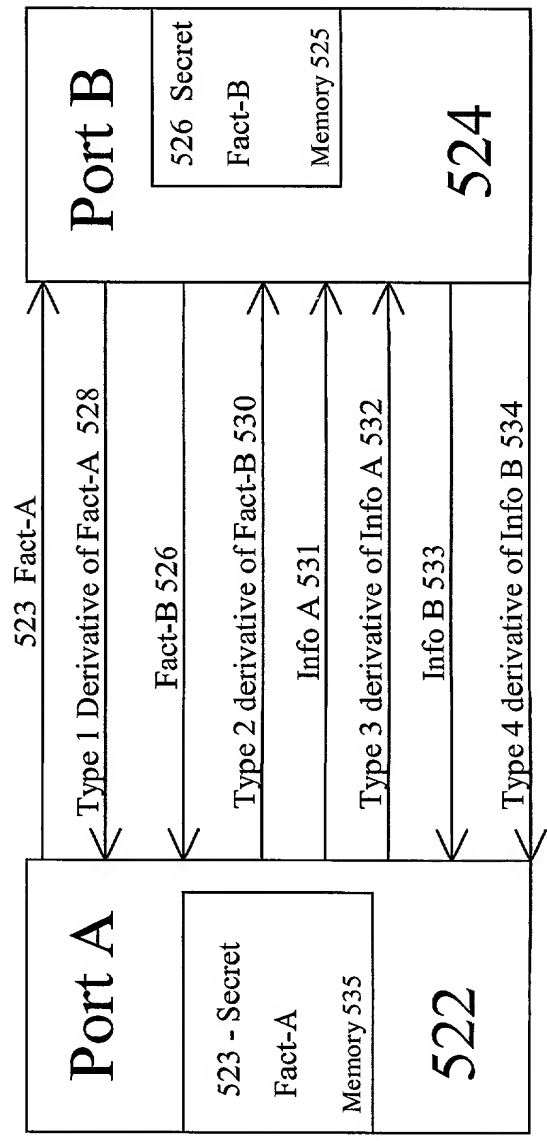


Figure 5d

| Step # | Name / Function | Payload |
|--------|---------------------------|---|
| 1 | Request Authentication | Secret Fact A |
| 2 | Acknowledge Request | Secret Fact B; Type 1 derivative of Secret Fact A; InfoB; Type 3-4 derivative of Info B |
| 3 | Confirm Authentication | Type 2 derivative of Secret Fact B; InfoA; Type 3-4 derivateve of InfoA |
| | | |

Figure 6

FIG. 9 is a flowchart illustrating a mutual authentication process between two switches, Switch A and Switch B. The process begins with Switch A initiating the process (901) by generating and storing a random number Ra (930). Switch A then sends a SLAP_Request [Ra] to Switch B (902). Switch B responds by generating and storing a random number Rb (905). Switch B then sends a SLAP_Acknowledge [Rb, Sb(Ra), Cb] to Switch A (906). Switch A verifies B's certificate (Cb) (907). If the verification fails (No), authentication fails. If the verification succeeds (Yes), Switch A verifies B's signature (Sb) (908). If the verification fails (No), authentication fails. If the verification succeeds (Yes), Switch A sends a SLAP_Confirm [Sa(Rb), Ca] to Switch B (909). Switch B then verifies A's certificate (Ca) (910). If the verification fails (No), authentication fails. If the verification succeeds (Yes), Switch B verifies A's signature (Sa) (912). If the verification fails (No), authentication fails. If the verification succeeds (Yes), Switch B sends a SLAP_Done to Switch A (913). Finally, both switches are mutually authenticated (914).

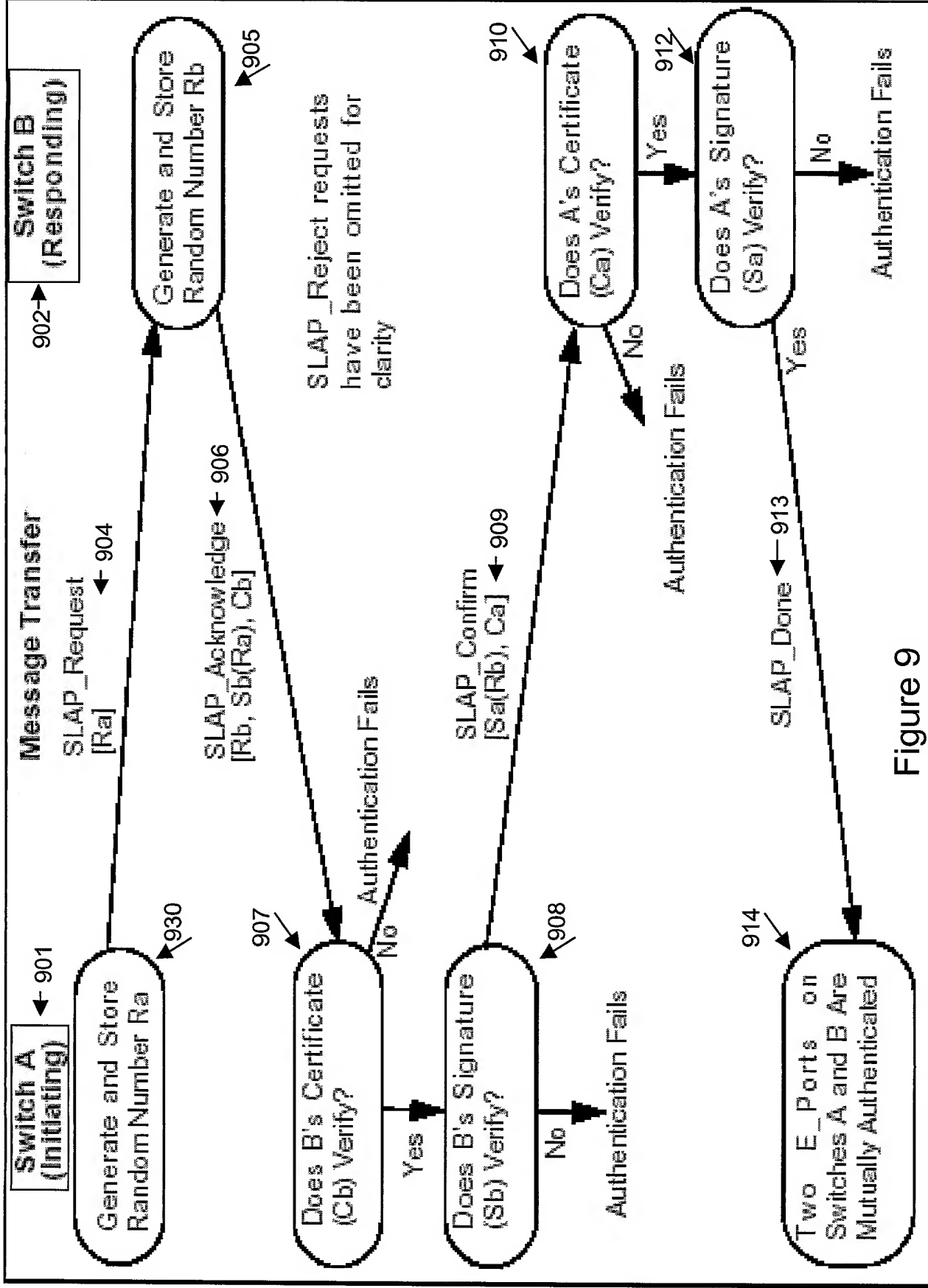


Figure 9

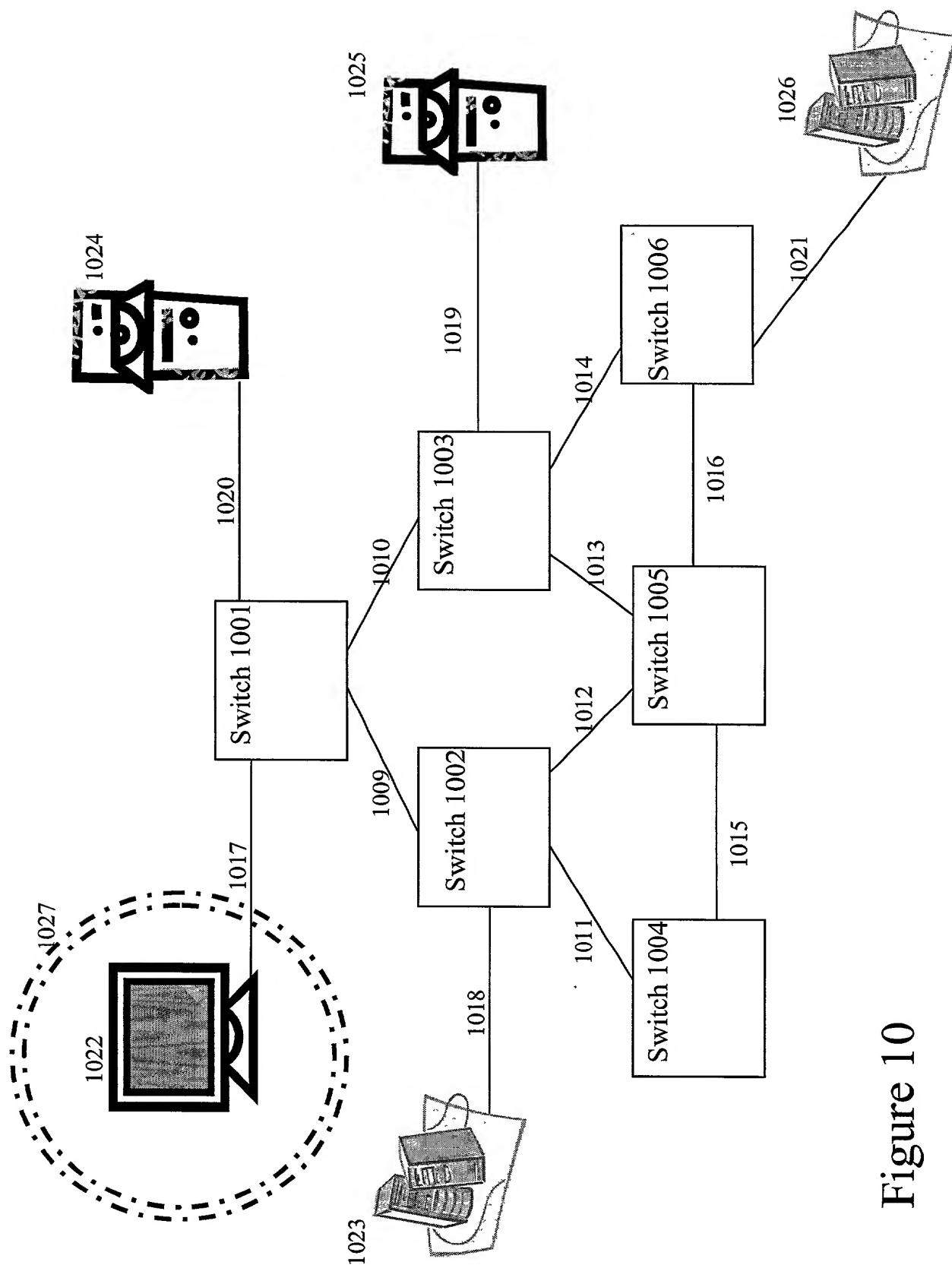


Figure 10

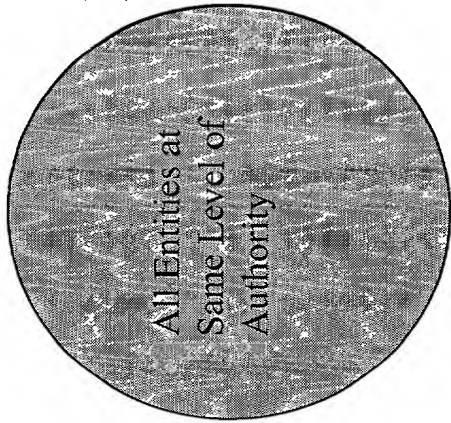


Figure
11a

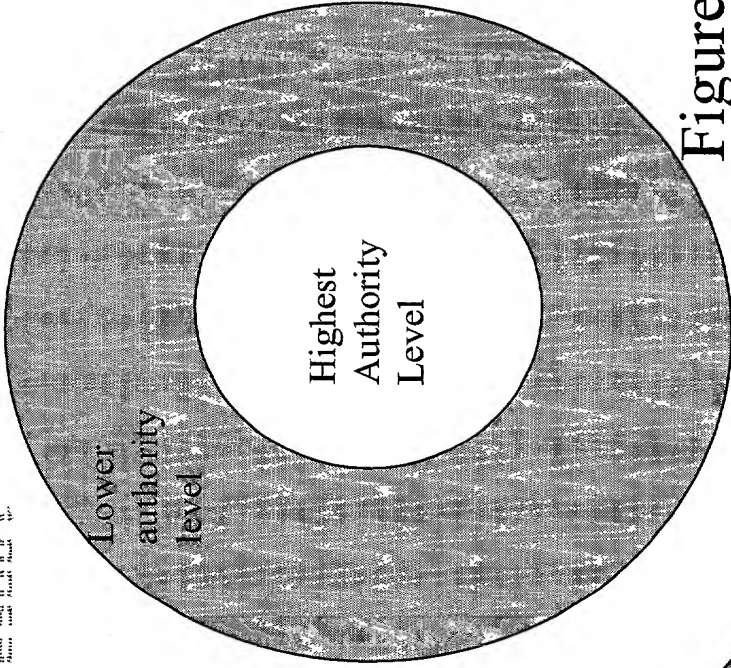


Figure
11b

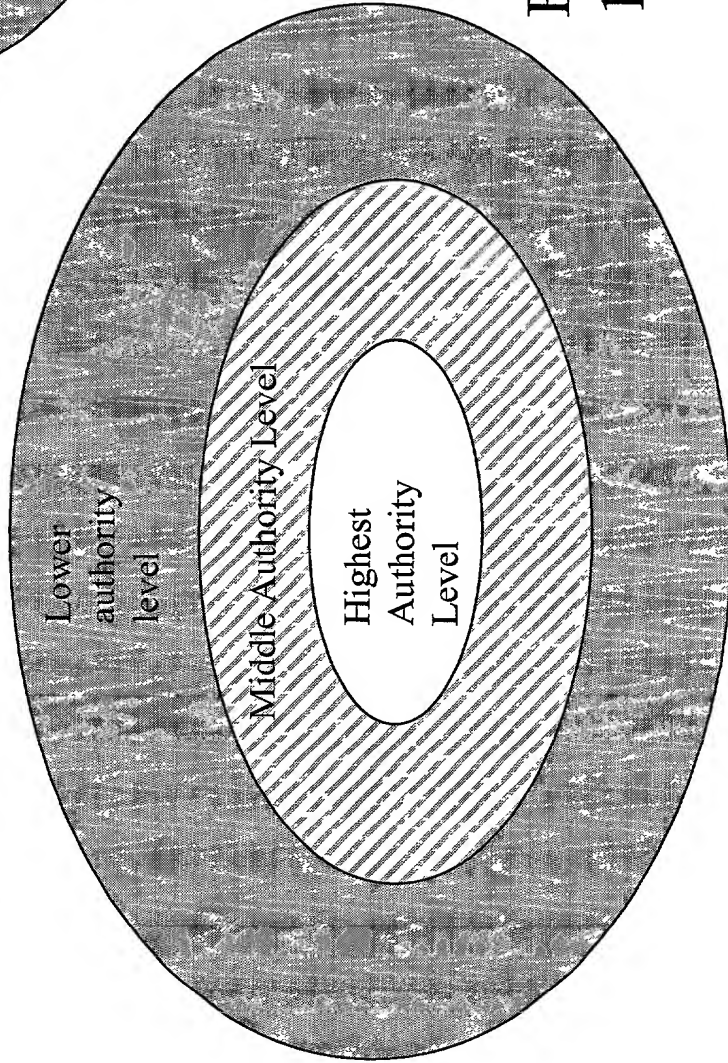


Figure
11c

FIG. 12 is a schematic diagram of a network system 1200. The network system 1200 includes a plurality of switches 1201, 1202, 1203, 1204, 1205, 1206, 1230, and 1231. The switches 1201, 1202, 1203, 1204, and 1205 are interconnected in a mesh topology. The switches 1206 and 1230 are connected to the switches 1203 and 1205, respectively. The switches 1231 and 1232 are connected to the switches 1203 and 1205, respectively. The network system 1200 also includes a plurality of endpoints 1221, 1222, 1223, 1224, 1225, and 1226. The endpoints 1221, 1222, 1223, 1224, and 1225 are connected to the switches 1201, 1202, 1203, 1204, and 1205, respectively. The endpoint 1226 is connected to the switch 1206. The network system 1200 is configured to provide network connectivity between the switches and the endpoints.

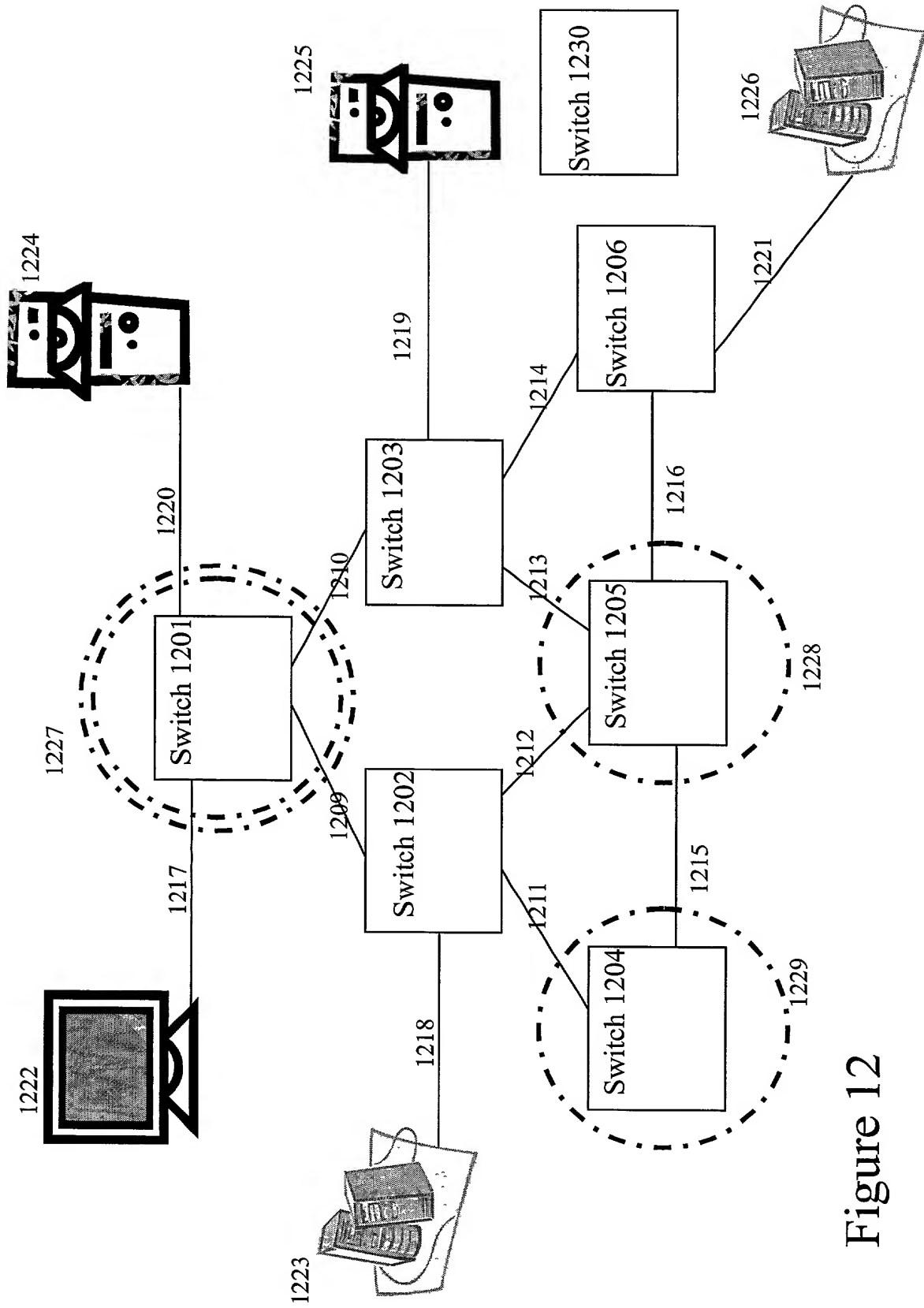


Figure 12

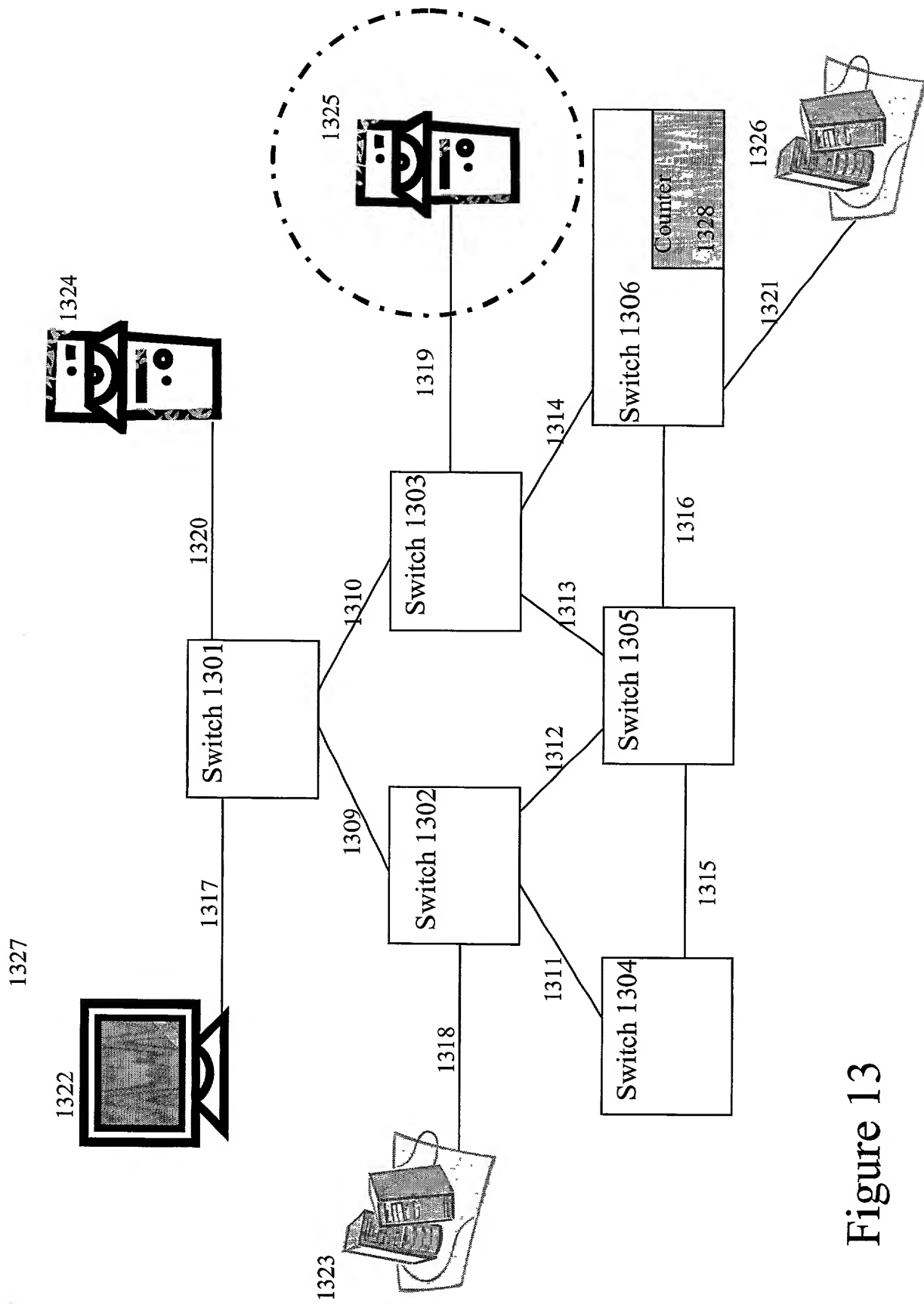
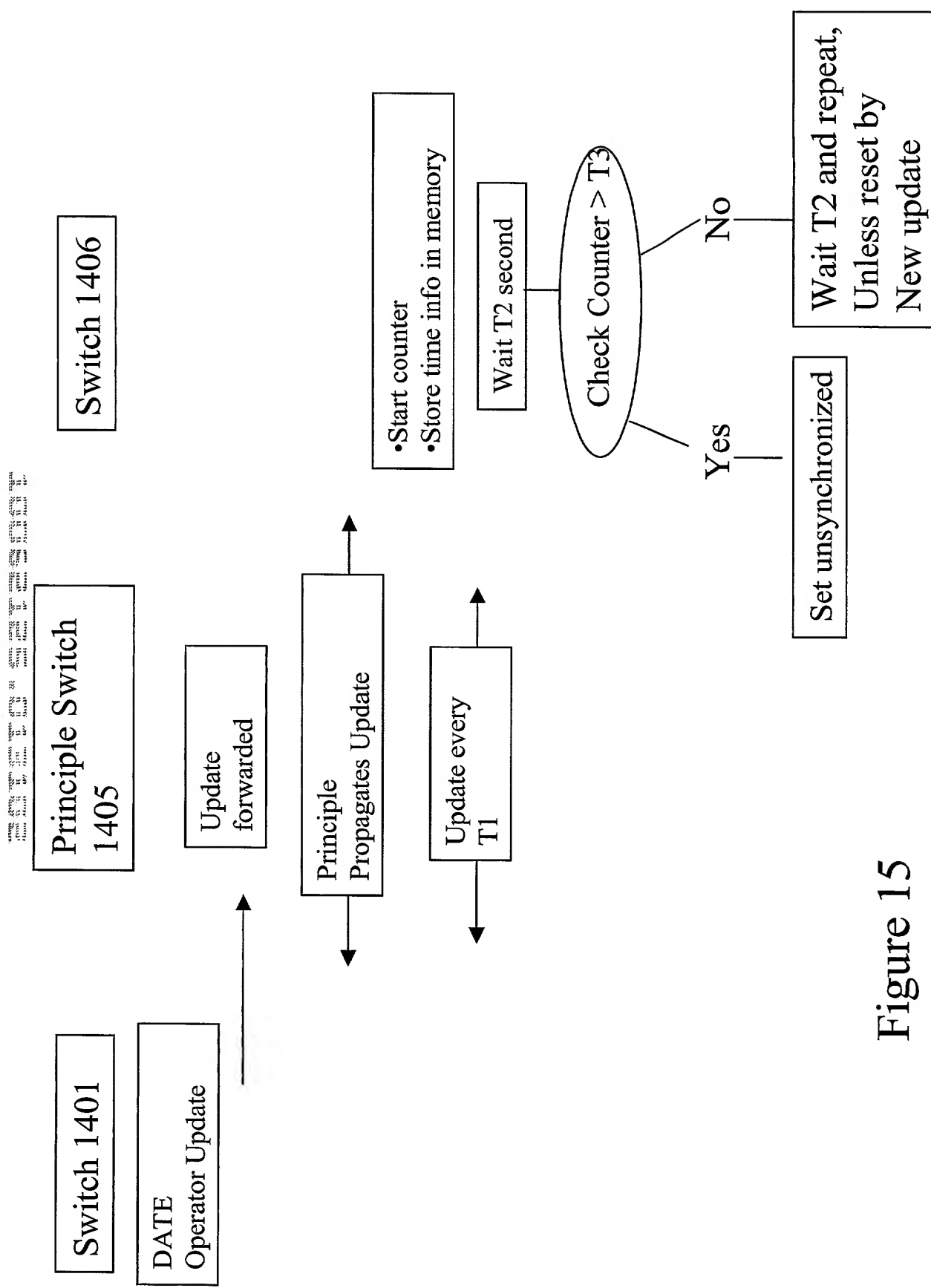


Figure 13



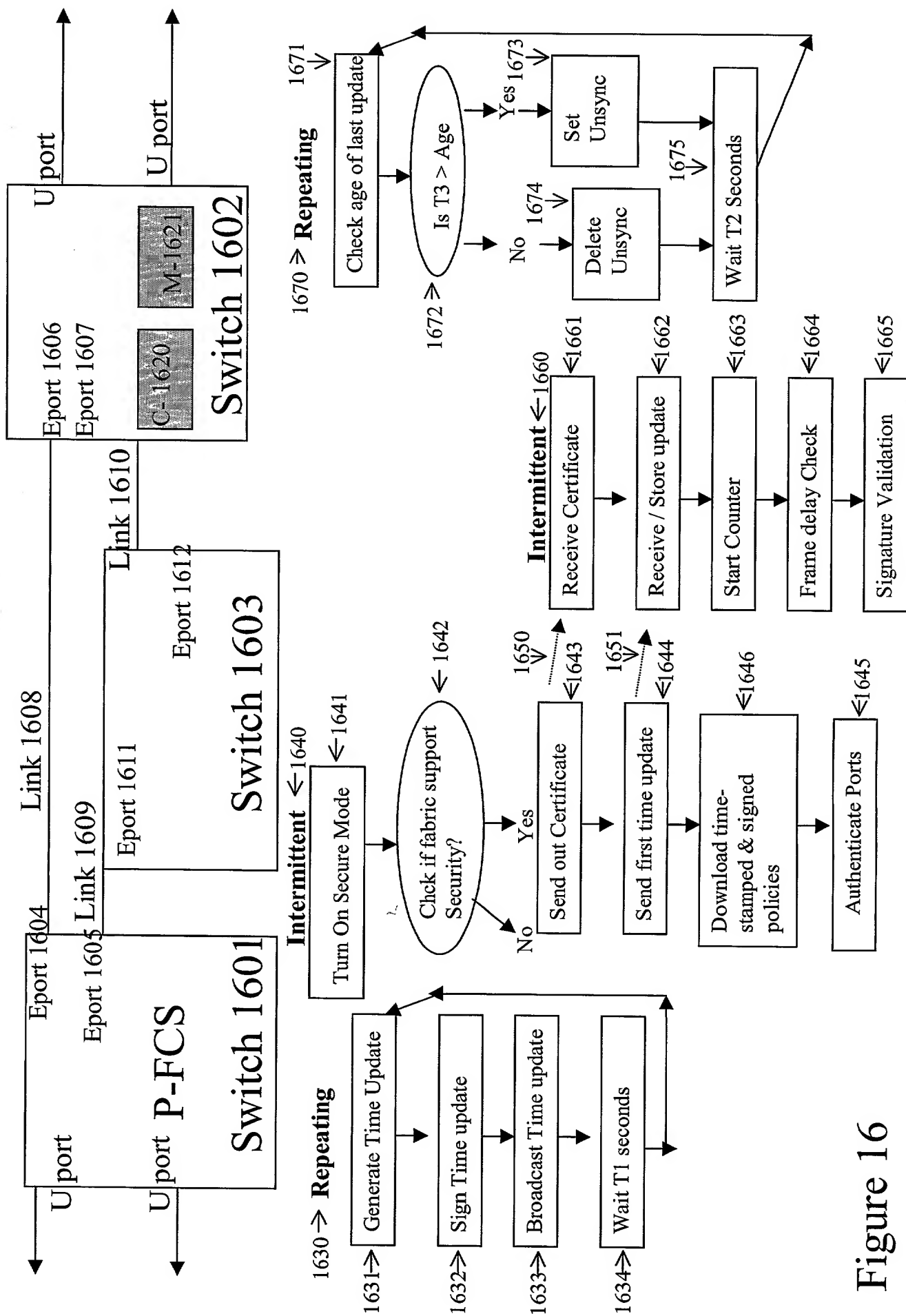


Figure 16